PATENTTI- JA REKISTERIHAL[redacted]US
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 3.7.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Corporation** **Helsinki**
Patenttihakemus nro Patent application no	**20025018**
Tekemispäivä Filing date	**23.04.2002**
Kansainvälinen luokka International class	**H04L**

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Keksinnön nimitys
Title of invention

"Järjestelmä digitaalisessa langattomassa tiedonsiirtoverkossa päästä päähän -salauksen järjestämiseksi ja vastaava päätelaite"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Marketta Tehikoski
Apulaistarkastaja

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

JÄRJESTELMÄ DIGITAALISESSA LANGATTOMASSA TIEDONSIIRTOVERKOSSA PÄÄSTÄ PÄÄHÄN -SALAUKSEN JÄRJESTÄMISEKSI JA VASTAAVA PÄÄTELAITE

Keksinnön kohteena on järjestelmä digitaalisessa langattomassa tiedonsiirtoverkossa päästä päähän (e2e) -salauksen järjestämiseksi, erityisesti audiomuotoiselle lähetykselle, jossa tiedonsiirtoverkossa viestii keskenään kaksi tai useampia päätelaitteita, joihin kuuluu ainakin

- koodekki analogisen audiosignaalin muuntamiseksi datavirraksi ja päin vastoin,
- ilmatiesalausvälineet,
- välineet päätelaitteen yhteyteen tallennettujen salausparametrien hallinnoimiseksi
- salausavaingeneraattori käyttöavaimen luomiseksi sanotuilla salausparametreilla,
- välineet datavirran salaamiseksi ja salauksen purkamiseksi luodulla käyttöavaimella,
- välineet salatun datavirran synkronoimiseksi ja synkronoinnin purkamiseksi ja
- ainakin yksi rajapinta salausparametrien vastaanottamiseksi tiedonsiirtoverkosta,

ja jossa ainakin yksi tiedonsiirtoverkkoon kuuluvista päätelaitteista on sovitettu toimimaan erityisenä palvelinpäätelaitteena, joka hallinnoi ja jakaa ainakin tiedonsiirtoverkkoa koskevia salausparametreja muille päätelaitteille asetetun kriteerin perusteella. Keksintö koskee myös järjestelmän toteuttavaa päätelaitetta.

TETRA (Terrestrial Trunked RAdio) on erityisesti vaativille ammattilais-käyttäjäryhmille suunniteltu digitaalinen, langaton ja yhteiskäyttöinen tietoliikennestandardi. TETRA-standardin mukaiselle järjestelmälle, jota jatkossa TETRA-järjestelmäksi kutsutaan on kehitetty erityisesti juuri esimerkiksi julkisten turvallisuusorganisaatioiden (poliisi, palolaitos, sairaankuljetus), julkista liikennettä ylläpitävien organisaatioiden (metro, rautatiet, lentoasemat, taksiliikenne) ja sotilaskäyttäjäryhmien tarpeita silmälläpitäen. Ominaista näille kaikille käyttäjäryh-

mille on niiden viestintäliikenteelle asettamat korkeat luotettavuus- ja turvallisuusvaatimukset.

TETRA-järjestelmä perustuu avoimiin standardeihin, jotka on kehittänyt ETSI (European Telecommunication Standard Institute) ja sen yhteydessä toimiva TETRA MoU (Memorandum of Understanding) -organisaatio.

TETRA-järjestelmälle on siis ominaista mm. sen käyttäjäkunnan asettamat suuret vaatimukset radioteitse suoritettavan liikennöinnin turvallisuudelle. Ilmarajapinnan ollessa tunnetusti hyvin haavoittuvainen kaikenlaiselle salakuuntelutoiminnalle, on kaikissa nykyaikaisissa langattomissa tietoliikennejärjestelmissä jossain muodossa pyritty huolehtimaan ilmarajapinnan tietoturvallisuudesta. Tällä tarkoitetaan päätelaitteen ja verkkoinfrastruktuurin välisen yhteyden turvaamista. Verkkoinfrastruktuurin sisällä tiedonsiirto tapahtuu luotettuna, koska järjestelmän fyysiseen rakenteeseen on ulkopuolisten tunkeutujien erittäin epätodennäköistä päästä käsiksi.

TETRA-järjestelmälle kehitettyä salaustapaa käytetään ensisijaisesti kahden avaintarpeen saavuttamiseksi. Ensimmäinen näistä on vahva tunnistusmekanismi ja toinen on radioliikenteen ilmarajapintasalaus.

TETRA-järjestelmässä salataan muutoin niin haavoittuvassa ilmarajapinnassa päätelaitteen ja tukiaseman välisen puhe- ja dataliikenteen lisäksi myös lähes kaikki signalointi-informaatio ja päätelaitteiden identiteettitunnisteinformaatio. Ilmarajapintasalaus perustuu avainlajitelmaan, jolla käyttäjä ja signaali-informaatio salataan ilmarajapinnan yli päätelaitteen ja TETRA SwMI:n (Switching and Management Infrastructure) välillä niin henkilökohtaisessa kuin ryhmäliikenteessäkin. Ilmarajapintasalaus tukee useita, hyviksi todettuja standardeja ja valmistajakohtaisia salausalgoritmeja.

Jokaisessa salausta käyttävässä järjestelmässä olettaen, että on valittu hyvät algoritmit ja protokollat, järjestelmän turvallisuus perustuu pohjimmiltaan salausavaimiin ja niiden generointi, jako-, käyttö- ja suojaustapoihin. TETRA-järjestelmässä käytetään ilmarajapintasalauksessa esimerkiksi GSM-järjestelmästä poiketen useampia salausavaimia riippuen käytettävästä yhteystyypistä. Yksilö-, ryhmä- ja DMO-yhteyksille (Direct Mode Operation) on kullekin omat salausavaimensa. Avaimien jako on järjestetty TETRA-järjestelmän ilmarajapintasalauksessa tapahtumaan OTAR-menetelmällä (Over the Air Re-keying), joka mahdollistaa järjestelmälle tavan vaihtaa avaimia päätelaitteiden haltijoiden toiminnan avainten jaosta sen enempää häiriintymättä.

Monissa tapauksissa ilmarajapintasalauksella luodaan riittävä luottamus tiedonsiirrolle ilman sen suurempia lisäturvallisuusjärjestelyjä. Kuitenkin TETRA-järjestelmässä on esimerkiksi tietyillä asiantuntijakäyttäjäryhmillä tarve erittäin korkean turvallisuustasoon. Esimerkkejä tällaisista ryhmistä ovat poliisin huumeyksiköt, valtiolliset rikostiedustelupalvelut ja sotilaskäyttäjäryhmät, jotka omaavat usein oleellisesti korkeamman, valtionhallinnollisesti asetetun turvallisuusluokituksen kuin tavanomainen pelkkää ilmarajapintasalausta käyttävä tiedonsiirtoverkko pystyy tarjoamaan. Tällöin lisäturvallisuus vaatimukset koskevat, ei pelkästään ilmarajapinnan yli vaan myös varsinaisessa verkkoinfrastruktuurissa tiedonsiirron suojaamista päätelaitteesta toiseen.

Nämä seikat luovat lisävaatimuksia esimerkiksi anonymiteetin ja edistyneemmän luottamuksellisuuden saavuttamiseksi. Anonymiteettivaatimus on tuettu TETRA-järjestelmän standardeissa turvallisuusmekanismeissa, mutta jälkimmäinen vaatimus täytetään päästä päähän -salauksella (end-to-end encryption, e2e), jota käytetään nimenomaan kaikkein suurinta tiedonsiirtoturvallisuutta vaativissa tilanteissa koko järjestelmän läpi päätelaitteesta päätelaitteeseen.

Kuvan 1 alalaidassa esitetyillä nuolilla kuvataan ilmarajapintasalauksen ja päästä päähän -salauksen eroa päätelaitteiden välisessä liikennöinnissä.

Esimerkiksi julkisilla turvallisuusorganisaatioilla on spesifiset, valtionhallinnollisesti korkeiksi asetetut turvallisuusvaatimukset päästä päähän -salauksen toteuttamiseksi, jotka eroavat esimerkiksi sotilaallisten käyttäjäryhmien turvallisuusvaatimuksista. Kaikkien tällaisten organisaatioiden on voitava määritellä oma päästä päähän -salausjärjestelmänsä näiden omien tarpeidensa mukaisiksi.

ETSI:n MoU-organisaatio on tuottanut suosituksen (SFPG Recommendation 2), jossa määritellään kaikki se, joka vaaditaan päästä päähän -salauksen toteuttamiseksi salausalgoritmien yksityiskohtia lukuun ottamatta. Algoritmit esitetään suosituksessa mustina laatikkoina. Koska tarkoituksena on tarjota myös yleisille, salauksen suhteen erityisen korkeita vaatimuksia asettamattomille käyttäjäryhmille täydellinen ratkaisu, on suositukseen sisällytetty liitteeksi esitys salausfunktioiden toteuttamisesta tunnettua IDEA-algoritmia (International Data Encryption Algorithm) käyttäen.

Puhdas tosiasia on kuitenkin se, että vaikka turvallisuustoimenpot onkin integroitu järjestelmään, niin tämä ei kuitenkaan takaa sitä, että järjestelmästä olisi saatu täysin turvallinen. Turvallisuusriskit saadaan tunnetulla tavalla toimittaessa pidettyä kuitenkin tiivistettyinä siten, että ne keskitetään järjestelmän tiettyihin elementteihin, joita voidaan sitten riittävällä tasolla valvoa.

Tämä valvonta on yksi turvallisuuden hallintaan liittyvistä työtehtävistä. Toisena tehtävänä on taata, että turvallisuusmekanismia käytetään kelvollisella tavalla ja että eri mekanismit on integroitu kelvollisella tavalla kaikenkattavan turvallisuusjärjestelmän saavuttamiseksi.

Ilmatiesalaus on TETRA-järjestelmässä tunnetun tekniikan mukaisesti kaikin puolin riittävä ja ongelmaton. Kuitenkin edellä esitetyistä turvallisuuteen liittyvistä tosiasioista huolimatta, ei päästä päähän -salauksen järjestämiseksi ole pystytty tarjoamaan tunnetulla tekniikalla täysin käyttäjäryhmäkohtaista toteutustapaa. Tämä on toivottu ominaisuus esimerkiksi juuri sanotuissa asiantuntijakäyttäjäryhmissä, joissa yleisenä trendinä nykyisin vallitsee ilmapiiri, että nämä haluavat pitää esimerkiksi salausavaimensa ja algoritminsa täysin omassa hallinnassaan, eivätkä halua luovuttaa esimerkiksi päätelaiteiden valmistajille mitään tietoa käyttämästään salausinformaatiosta.

Nykyisessä toimintatavassa ovat esimerkiksi päätelaitteiden valmistajat vahvasti tekemisissä salaukseen liittyvien moduulien, kuten esimerkiksi salausalgoritmien ja avaingeneraattorien toteutuksessa. Lisäksi esimerkiksi salausalgoritmien päivittäminen päätelaitteisiin on nykyisin käytännössä erittäin hankalaa ellei jopa mahdotonta, koska ne on saatettu toteuttaa jopa laitteistotasolla.

Dynaamisia toteutuksia salauksen järjestämiseksi tiedonsiirrossa tunnetaan ainakin PC-ympäristöstä. Näissä kuitenkin käsitellään yleensä dataliikennettä, jolloin tätä tekniikkaa ei pystytä hyödyntämään langattomassa ja voice-ympäristössä.

US-julkaisussa 5,528,693 on esitetty puhemuotoisen tiedonsiirron salausta. Tämä ei kuitenkaan ole esimerkiksi salausalgoritmien hallinnaltaan dynaaminen, jolloin päätelaitteessa on käytössä aina kiinteät salausalgoritmit.

Tämän keksinnön tarkoituksena on saada aikaan uudenlainen järjestelmä ja vastaava päätelaite päästä päähän -salauksen järjestämiseksi, joka parantaa oleellisesti salauksen tarvitsijan eli käyttäjäryhmän ja päätelaitteen valmistajan toiminta-edellytyksiä. Keksinnön mukaisen järjestelmän tunnusomaiset

piirteet on esitetty patenttivaatimuksessa 1 ja vastaavan päätelaitteen patenttivaatimuksessa 5.

Keksinnön mukainen järjestelmä muuttaa päästä päähän -salauksen rakenteellisuutta siten, että osa salauksen komponenteista ulkoistetaan kuitenkin itse varsinaisen salauksen pysyessä mahdollisesti jopa ennallaan. Rakenteellisuuden muutoksella ja ulkoistuksella saadaan oleellisesti parannettua salauksen turvallisuustasoa ja saavutetaan lisäksi se, että esimerkiksi päätelaitteen valmistajan ei tarvitse enää huolehtia käyttäjäryhmien asettamista vaatimuksista salauksen järjestämisen suhteen.

Keksinnön mukaisessa järjestelmässä päätelaitteelle on järjestetty dynaaminen suoritinympäristö, jolla voidaan ajaa sille spesifioituja sovelluksia. Järjestelmässä päätelaitteelle ladataan erään edullisen suoritusmuodon mukaisesti tiedonsiirtoverkon kautta korkean turvallisuustason omaavaa viranomaismateriaalia, jotta päätelaite voisi suoriutua sille asetetuista tehtävistään. Tällainen materiaali voi käsittää esimerkiksi päästä päähän -salausinformaatiota, kuten avaimia ja salaussovelluksia.

Erään edullisen suoritusmuodon mukaan päätelaitteelle sovitettu suoritin on Java®-pohjainen ja spesifioitu J2ME:n mukaiseksi (Java 2 Platform Micro Edition).

Tiedonsiirtoverkkoon, joka voi olla esimerkiksi FDMA- (Frequency Division Multiple Access), TDMA- (Time Division Multiple Access), CDMA- (Code Division Multiple Access) tai johonkin muuhun langattomaan tekniikkaan perustuva, on järjestetty erityinen päätelaite, jolla hallinnoidaan salausinformaation, kuten esimerkiksi juuri salaussovellusten ja -avaimien jakoa.

Keksinnön mukaisessa järjestelmälle on ominaista salauksen suorittaminen päätelaitteella ohjelmallisesti. Tunnetun teknii-

kan mukaiseen laitteistotasolla tapahtuvan salaukseen verrattuna tällä saavutetaan päätelaitteiden salaussovelluksien dynaamisuus, jolloin sovelluksia voidaan päivittää erityisen vaivattomasti.

Salausinformaation päivitys voidaan erään suoritusmuodon mukaan suorittaa siten, että päätelaitteen käyttäjältä ei edellytetä sen suhteen mitään toimenpiteitä eikä hänen toiminta päivitystoimenpiteiden johdosta mitenkään häiriinny.

Vielä eräänä lisäetuna päätelaitteella ajettavalla dynaamisella sovelluksella tarjotaan esimerkiksi päätelaitteeseen sovitetulle toimikortille komentojoukko, jolla se voi ohjata päätelaitetta dynaamisen sovelluksen ohjelmointirajapinnan kautta.

Toisaalta vielä eräänä keksinnön mukainen järjestelmän hyötynä päätelaitteen valmistajan näkökulmasta saavutetaan se, että päätelaitteeseen ei ole kiinteästi tallennettu mitään sellaista päästä päähän -salausinformaatiota, josta ei päätelaitteen valmistajalla olisi tietoa.

Muut keksinnön mukaiselle järjestelmälle ominaiset piirteet käyvät ilmi oheisista patenttivaatimuksista ja lisää saavutettavia etuja on lueteltu selitysosassa.

Keksinnön mukaista järjestelmää, jota ei ole rajoitettu seuraavassa esitettäviin suoritusmuotoihin, selostetaan tarkemmin viittaamalla oheisiin kuviin, joissa

Kuva 1 esittää ilmatiesalausta ja päästä päähän -salausta tiedonsiirtoverkossa,

Kuva 2 esittää erästä esimerkkiä keksinnön mukaisen järjestelmän toteuttavasta päätelaitteesta ja palvelimesta kaaviokuvana,

Kuva 3 esittää erästä esimerkkiä keksinnön mukaisen järjestelmän ohjelmointirajapinnoista salauksen käyttöparametrien hallinnassa ja

Kuva 4 esittää erästä esimerkkiä keksinnön mukaisen järjestelmän ohjelmointirajapinnoista salausjärjestelmän hallinnassa.

Kuvassa 1 on esitetty kaaviokuvana ilmatiesalauksen ja päästä päähän -salauksen periaate-erot tiedonsiirtoverkossa, kuten esimerkiksi digitaalisessa, langattomassa TETRA-standardin mukaisessa verkossa 10.

Alan ammattimiehelle on ilmeistä se, että vaikka keksinnön mukaista järjestelmää kuvataankin tämän sovellusesimerkin yhteydessä juuri TETRA-infrastruktuuriin perustuvassa tiedonsiirtoverkossa 10, niin keksinnön mukaisen järjestelmän ja sitä vastaavan päätelaitteen käyttö ei ole kuitenkaan rajoitettu juuri tähän järjestelmään. Yleisesti todettakoon, että järjestelmää ja sitä vastaavaa päätelaitetta voidaan soveltaa yleensäkin digitaalisissa, langattomissa verkkojärjestelmissä, kuten esimerkiksi FDMA-, CDMA-, TDMA-tekniikat ja näiden alimääritte-lyt.

Ilmatiesalauksessa (Air-interface encryption) radiosignaali välittyy tiedonsiirtoverkossa 10 salattuna vain langattoman päätelaitteen 11.1 ja tiedonsiirtoverkon 10 infrastruktuuriin kuuluvan tukiaseman 16.1 sekä tukiaseman 16.3 ja langattoman päätelaitteen 11.2 välillä. Varsinaisessa verkkoinfrastruktuurissa (reitittimiä, siltoja, toistimia, keskuksia ym. alan ammattimiehelle ilmeistä laitteistoa) 16.1, 18.2, 17, 18.1, 16.3 tiedonsiirto tapahtuu luotettuna (trusted). Tällä tarkoitetaan esimerkiksi sitä, että ulkopuolisilta eli mahdollisesti juuri vakoilua suorittavilta tahoilta estetään fyysinen pääsy verkkoinfrastruktuurin 10 muodostavien laitteiden 17, 18.1, 18.2 ja näiden välisten tiedonsiirtoväylien yhteyteen.

Päästä päähän -salauksessa (End-to-End encryption) signaali kulkee salattuna koko välin lähettävältä päätelaitteelta 11.1 aina lähetyksen vastaanottavalle päätelaitteelle 11.2. Tiedonsiirtoverkolla 10 on tällöin pelkästään datan kuljettajan osa.

On huomattava, että standardeja, ilmarajapintasalauksessa käytettyjä salausmekanismeja käytetään lisäksi myös päästä päähän -salauksessa. Ilmarajapintasalauksella ei päätelaitteen 11.1, 11.2 ja infrastruktuurin 10 välillä salata pelkästään puhetta vaan myös signaali.

Edelleen verkkoon 10 saattaa olla liittyneenä mainittujen langattomien päätelaitteiden 11.1, 11.2 lisäksi erilaisia muita tiedonsiirtolaitteita, kuten tiedonsiirtoverkkoja toisiinsa yhdistäviä yhdyskäytäviä Gateway 13, operaattorin työasemia DT 14, joilla esimerkiksi hallitaan käyttäjäryhmien muodostamista ja ohjataan niiden toimintaa, linjaliitännäisiä päätelaitteita LCT 12 ja salausparametrien ja salauksen hallinnointia keksinnön järjestelmän mukaisesti suorittavia erityisiä palvelinpäätelaitteita KMC 15.

Kuvassa 2 on kuvattu toiminnallisuudet ja niiden väliset yhteydet, jotka toteuttavat erään keksinnön mukaisen järjestelmän suoritusmuodon langattomassa päätelaitteessa 11.1, 11.2 ja salauksen hallinnointia tiedonsiirtoverkossa 10 suorittavassa erityisessä palvelinpäätelaitteessa 15.

Kyseinen erityinen palvelinpäätelaite 15 voi olla esimerkiksi tiedonsiirtoverkkoon 10 liittynyt datapääte, jonka yhteyteen on järjestetty tallennusvälineet dB ainakin sinänsä tunnettujen salausparametrien 19 ja sovelluksien, erityisemmin dynaamisten salaussovelluksien 32 säilyttämiseksi. Palvelinpäätelaite 15 on järjestetty erityisen tietoturvalliseksi, koska sillä säilytetään tiedonsiirtojärjestelmän kannalta kriittistä informaatiota.

Sanottuihin salausparametreihin 19 voidaan luetella kuuluviksi esimerkiksi OTAK-menetelmällä (Over the Air Keying) päätelaitteille 11.1, 11.2 enemmän tai vähemmän säännöllisin väliajoin vaihdettavat ja välitettävät salausavaimet, salauksen ohjausparametrit ja muut vastaavat sinänsä tunnetut salausparametrit.

Sovelluksien 32 tallennusmediaan dB on järjestetty päätelaitteille 11.1, 11.2 tiedonsiirtoverkon 10 välityksellä siirrettävissä olevia sovelluksia, kuten esimerkiksi salausavainvirran generointiin tai varsinaisen datavirran salaukseen käytettäviä algoritmeja. Sovellukset 32 voivat olla erään edullisen sovellusmuodon mukaan JAVA®-sovelluksia, erityisemmin J2ME-spesifikaation mukaisia (Java 2 Platform Micro Edition). Myös muut sovelluksien esitysmuodot, kuten ilman tulkkausta suoritettavissa oleva puhdas natiivikoodi, Chet, C#, BREW soveltuvat käytettäviksi.

Erityiselle palvelinpäätelaitteelle 15 on lisäksi järjestetty hallinnointitoiminnallisuus 34, jolla hoidetaan salausparametrien ja -sovelluksien 19, 32 hallinnointia ja ohjataan niiden jakelua päätelaitteille 11.1, 11.2 asetetun kriteerin mukaisesti.

On huomattava, että palvelintoiminnallisuutta tarjoava päätelaite 15 voidaan toteuttaa millä tahansa TETRA-verkon 10 päätelaitteista, jos näille on järjestetty resurssit salausavaimien ja -sovelluksien 19, 32 hallitsemiseksi ja jakamiseksi.

Päätelaitteen 11.1, 11.2 ollessa kytkeytyneenä sinänsä tunnetunlaisen ilmarajapinta protokollan 19 välityksellä tiedonsiirtoverkkoon 10, se voi vastaanottaa sanottuja salausparametreja ja -sovelluksia 19, 32 palvelinpäätelaitteelta 15 valittua siirtokanavaa ja edullisemmin valittua salaustapaa käyttäen, joiden käyttö ei välttämättä tarvitse olla kiinteästi määritelty.

Eräs edullinen esimerkki tällaisesta siirtokanavana käytettävästä jakelutavasta ovat esimerkin mukaisessa TETRA-verkossa 10 salatut SDS-viestit. SDS (Short Data Service) on lyhytsanomaviestityyppi, joka välittyy päätelaitteen 11.1, 11.2 läpi suoraan sen yhteyteen järjestetylle toimikortille, kuten esimerkiksi SIM-moduulille (Subscriber Identity Module) siten, että päätelaite 11.1, 11.2 ei tulkkaa viestiä millään tavalla. Muita esimerkkejä toimenpiteeseen käytettävistä siirtokanavista on SMS-viestit (Short Message System) ja GSM-data.

Sovelluksien 32 lataus päätelaitteille 11.1, 11.2 voidaan suorittaa myös paikallisesti. Tämä tapahtuu esimerkiksi siten, että salausinformaatiota 19, 32 vastaanottava päätelaite 11.1, 11.2 on kiinteästi kytketty sanottuun palvelinpäätelaitteeseen 15, josta sitten siirretään salausinformaatiota ja -sovelluksia 19, 20 esimerkiksi sarjaliikennemuotoisesti, IrDA- (Infrared Data), Bluetooth-yhteydellä tai jotain muuta päätelaitteelle 11.1, 11.2 edullista tiedonsiirtoväylää pitkin (ei esitetty).

Keksinnön mukaisessa järjestelmässä on päätelaitteen 11.1, 11.2 yhteyteen järjestetty esimerkiksi informaation joustavan käsittelyn mahdollistava toiminnallisuus, joka erään edullisen suoritusmuodon mukaan voidaan toteuttaa esimerkiksi SIM-moduulilla 28. SIM-moduulin 28 muistivälineisiin järjestettyyn e2e -osioon 23 tallennetaan palvelinpäätelaitteelta 15 ladatut ja puretut salausavaimet ja -sovellukset 19, 32, kuten esimerkiksi käyttöavaingeneraattori.

Näitä toimenpiteitä varten on SIM-moduulin 28 yhteyteen järjestetty SAT-osio 21 (SIM Application Toolkit). SAT-osio 21 tarjoaa päätelaitteen 11.1, 11.2 ja SIM-moduulin 28 välille mekanismin, joka mahdollistaa SIM-moduulille 28 järjestetyn sovelluksen vuorovaikuttaa ja ohjata päätelaitteen 11.1, 11.2 toimintaa edellyttäen, että päätelaite 11.1, 11.2 tukee SAT mekanismia. SAT-osion 21 komentokirjastolla suoritetaan keksinnön mukaisen järjestelmässä salausavaimien ja -sovelluksien 19, 32 vastaanot-

tamista, näiden salauksen purkamista ja tallettamista SIM-moduulille 28 e2e -osioon 23.

Sujuvien päivitystoimenpiteiden lisäksi SAT-osion 21 komentokirjastolla pystytään tehokkaasti hallinnoimaan sanottua salausdataa ja ohjaamaan SIM-moduulilta 28 käsin päätelaitteeseen 11.1, 11.2 järjestettyä, tuonnempana kuvattua salaustoiminnallisuutta. SAT-osio 21 edellyttää päätelaitteelta 11.1, 11.2 SAT-yhteensopivuutta, jolloin sanottujen SIM-moduulille 28 järjestettyjen sovelluksien on oltava päätelaitteen 11.1, 11.2 ymmärtämässä muodossa ja päätelaitteen 11.1, 11.2 on kyettävä toteuttamaan sovelluksien sille antamia komentoja.

Salausavaimien 19 ja salauksessa käytettävien sovelluksien 32 (avaingeneraattori, KSG) päivitys suoritetaan siis erään keksinnön sovellusmuodon mukaisesti päätelaitteen 11.1, 11.2 SIM-moduulille 28. SIM-moduulin 28 ohjelmistoympäristö voi perustua esimerkiksi J2ME-spesifikaatioon, joka on yhteensopiva SAT-ohjelmistorajapinnan kanssa.

Edelleen SIM-moduulin 28 SAT-osion 21 tarjoamiin ominaisuuksiin kuuluu SIM-moduulille 23 tallennettujen monitasoisten valikkojen ja niiden taakse järjestettyjen yksinkertaisten sovelluksien tai toimintojen hyödyntämismahdollisuus päätelaitteessa 11.1, 11.2.

Keksinnön mukaisessa järjestelmässä on päätelaitteelle 11.1, 11.2 järjestetty edelleen sovellushallinnointi 22. Tämä voidaan erään edullisen sovellusmuodon mukaan toteuttaa esimerkiksi JAM:lla (Java Application Management). Sen tehtävä on toimia rajapintana päätelaitteen 11.1, 11.2 RTOS:n (Real Time Operating System), SIM-moduulille 28 järjestetyn päätelaitetta 11.1, 11.2 komentavan sovelluksen mahdollistavan SAT-osion 21 ja KVM:n eli Java®-virtuaalisuorittimen 20 välillä. JAM:lla 22 hallitaan päätelaitteelle 11.1, 11.2 ladattujen sovelluksien 32 pinoa ja niiden latausta virtuaalisuorittimelle KVM 20.

Päätelaitteen 11.1, 11.2 RTOS:n päällä ajetaan siis esimerkiksi Java® virtuaalisuoritinta KVM 20 (Kilobyte Java Virtual Machine), joka on edullisemmin J2ME-spesifikaation (Java 2 Platform Micro Edition) mukainen. Tällöin suoritin 20 on konfiguroitu edullisemmin MIDP-spesifikaation (Mobile Information Device Profile) mukaiseksi, jolloin KVM 20 tulee toimeen minimimäärällä luokkakirjastoja ja tarvittavia API:ja (Application Protocol Interface). JAM 22 huolehtii rajapintatoiminnasta yhdessä SIM-moduulin 28 SAT-osion 21 kanssa eli sen tehtävä on KVM:n 20 puolesta ohjata salaussovellusten 32 tallentamista, noutamista ja palauttamisesta päätelaitteen 11.1, 11.2 muistivälineiden, SIM-moduulin 28 e2e-osion 23 ja KVM:n 20 välillä. Lisäksi JAM:lla 22 kontrolloidaan Java®-sovellusten eli MIDdlettien lataamista tiedonsiirtoverkosta 10 (pistenuoli).

Päätelaitteen 11.1, 11.2 käyttäjätasolla on sinänsä tunnetunlainen analoginen audio-osa 25, johon kuuluvat ainakin mikrofonivälineet 25.2 käyttäjän puheen vastaanottamiseksi ja kaiutinvälineet 25.1 päätelaitteella 11.1, 11.2 vastaanotetun lähetyksen kuuntelemiseksi. Audiosignaalille tehdään audio-osan 25 digitaaliseen lohkoon sijoitetussa puhekoodekissa 24 AD-muunnos (encoding) sinänsä tunnetulla tavalla, josta on seurauksena salattava datavirta. Vastaavasti vastaanottaessa lähetystä salauksesta puretulle datavirralle suoritetaan puhekoodekissa 24 DA-muunnos (decoding), jotta se olisi kaiutinvälineiden 25.1 kautta ymmärrettävästi päätelaitteen 11.1, 11.2 käyttäjän kuultavissa.

Edelleen päätelaitteeseen 11.1, 11.2 kuuluu liitäntärajapinta ulkoiselle datapäätelaitteelle (DTE) 26, jolla salausinformaatiota, kuten avaimia ja sovelluksia voidaan ladata päätelaitteelle 11.1, 11.2 palvelinpäätelaitteelta 15 tai vastaavalta ilman yhteyttä varsinaiseen tiedonsiirtoverkkoon 10.

Kuvassa 3 on esitetty kaaviokuva eräästä keksinnön mukaisen järjestelmän edullisesta toteutustavasta käyttöparametrien kontrollissa rajapintakuvauksena. Kuvassa viivoitetulla alueella

kuvataan Java®-MIDdlettinä 27 toteutettavaa osaa, jota siis päätelaitteen RTOS:n päällä KVM:llä 20 ajetaan dynaamisesti. MIDdletin 27 toimintaa kuvataan seuraavassa ensin lähetettävän liikenteen näkökulmasta ja sen jälkeen vastaanotettavan liikenteen näkökulmasta.

MIDdlettin 27 yhteyteen on sovellusesimerkissä järjestetty kaksi toiminnallista API-rajapintaa. Ensimmäinen rajapinta on audio API 29, jonka takana on käyttäjärajapintaan järjestetty audio-osa 25 (mm. mikrofoni 25.2, kaiutin 25.1), puhekoodekki 24 ja muu alan ammattimiehelle ilmeinen toiminnallisuus, jota ei kuvassa ole esitetty. API määrityksessä on keksinnön kannalta oleellista koodekilta 24 MIDdlettiin 27 tuleva ja MIDdletistä 27 koodekille 24 lähtevä salaamaton datavirta (plain traffic).

Keksinnön mukaisessa järjestelmässä AD-muunnettu datavirta (plain traffic) siepataan siis käyttäjätason audio API:sta 29 ja syötetään päätelaitteen 11.1, 11.2 suorittimella eli KVM:llä 20 ajettavalle Java®-MIDdlet salaussovellukselle 27 prosessoitavaksi. Sovellus 27 toteuttaa esimerkiksi XOR-operaation tai jonkin muun valitun ja keksinnön järjestelmän mukaisesti päätelaitteelle 11.1, 11.2 saatetun salaussovelluksen.

Toinen rajapinta Java®-MIDdlettiin 27 on SIM API 28.1, jonka takana on esitetty SIM-moduulin 28 e2e-osiolle 23 keksinnön kannalta oleelliset toiminnallisuudet ja siellä säilytettävät salausparametrit. SIM-moduulin 28 e2e-osiossa 23 ajettavalle avaingeneraattorille KSG annetaan syötteenä salattaessa datavirtaa liikenteen salausavain TEK (Traffic Encryption Key) ja salauksen synkronoinnin suorittamiseksi lukuarvo IV (Initialation Vector).

Salausavain on palvelinpäätelaitteen 15 päätelaitteelle 11.1, 11.2 toimittama ja IV luodaan päätelaitteella 11.1, 11.2 tunnetun tekniikan mukaisesti. Avaingeneraattori KSG tuottaa käyttöavainjonoa, joka SIM API:n 28.1 kautta ohjataan MIDdlettiin 27

salaussovellukselle XOR. Lisäksi avaingeneraattori KSG tuottaa synkronointikehyksen (Synch frame), joka SIM API:n 28.1 kautta annetaan MIDdletillä 27 aikaan saadulle synkronointi toiminnallisuudelle 33.1 (Synch Control).

SIM-rajapinnan 28.1 eräänä toisena toteutusvaihtoehtona on serialport API. Tällöin päätelaitteen 11.1, 11.2 ulkoiseen liitinrajapintaan on sovitettu salausmoduuli, joka voi olla esimerkiksi sen akun yhteydessä. Tällöin avaingeneraattorin KSG hallintainformaatio voidaan osoittaa kyseiseen liitinrajapintaan. Edelleen salausmoduulilla tuotettua käyttöavainjonoa on myös mahdollista lukea ulkoisesta liitinrajapinnasta XOR ja/tai XOR' -operaatioille.

Edelleen päätelaite 11.1, 11.2 voi olla toteutettu myös siten, että sen ulkoiseen rajapintaan (esim. serialport API) ei ole kytketty salaustoiminnallisuuden tarjoavaa salausmoduulia eikä päätelaitteeseen 11.1, 11.2 kuulu myöskään SIM-moduulia 28. Tällöin keksinnön mukainen päästä päähän -salaustoiminnallisuus voidaan toteuttaa siten, että edellä kuvatussa sovellusesimerkissä SIM-moduulille 28 järjestetty salaustoiminnallisuus 23 on toteutettu myös ladattavana sovelluksena. Tällöin on varmistettava erityisesti päätelaiteen 11.1, 11.2 turvallisuudesta huolehtiminen.

XOR-operaatiolla salattua datavirta syötetään edelleen MIDdletin 27 suorittamalle synkronoinnin hallinnalle Synch Control. Sillä suoritetaan datavirralle sinänsä tunnetut toiminnot. Synch Control:sta salattu datavirta (crypt traffic') ja synkronointikehys (synch frame) poistuvat MIDdletistä audio API 29 rajapinnan kautta MAC-kerrokselle (Medium Access Control) ja edelleen fyysiselle kerrokselle 30.

MAC-kerroksessa hallitaan radiotaajuuksia ja aikavälejä (timeslots) sekä suoritetaan kehyksien varastus synkronointia varten. Fyysisessä kerroksessa suoritetaan sinänsä tunnetut toimenpi-

teet, kuten esimerkiksi datavirran koodaus ja dekoodaus (ilmarajapintasalaus/purku) ja edelleen lähetys/vastaanotto. Edelleen salattu data lähetetään tiedonsiirtoverkkoon 10, jossa se siirtyy sinänsä päästä päähän -salausteknisesti tunnetulla tavalla vastaanottavalle päätelaitteelle 11.2. Jos kehyksien varastus tehdään Synch Control:issa, niin synch frame, synch frame' -rajapintoja ei tarvita.

Lähetettävän ja vastaanotettavan salatun datavirran synkronisoiminen järjestetään päätelaitteen 11.1, 11.2 muistivälineillä joko puskuroituna tai toinen tapa on suorittaa se vuonohjausprotokollalla. Tällä varmistetaan, että päätelaitteelta 11.1, 11.2 verkkoon 10 ja verkosta 10 päätelaitteelle 11.1, 11.2 siirrettävät paketit (uplink/downlink-liikenne) ovat oikeassa järjestyksessä ja ajassa.

Päätelaitteen 11.1 vastaanottaessa e2e-lähetystä salattu datavirta (crypt traffic') ja synkronointikehys (synch frame') vastaanotetaan MIDdlettiin 27 audio API 29 rajapinnan kautta päätelaitteen 11.1 fyysisestä kerroksesta 30. Datavirran synkronointi puretaan sitä varten MIDdlettiin 27 järjestetyllä toiminnallisuudella (Synch Detect) 33.2. Synkronoinnin perusteella valitaan käytettävä purkuavain ja -algoritmi.

Salattu datavirta (crypt traffic) johdetaan XOR operaation käänteistoiminnon XOR' suorittavalle algoritmille ja salauksen purkamiseen vaadittava salausavain KSS saadaan esimerkiksi SIM-moduulin 28 e2e-osion 23 salausavaingeneraattorista KSG, jolle syötteenä annetaan TEK ja Synch Detect:stä 33.2 saatu Synch frame'. Edelleen purettu datavirta (plain traffic) johdetaan audio API:n 29 kautta päätelaitteen 11.1 audio osaan 25 ja tunnettujen välivaiheiden (mm. DA-muunnos) jälkeen saatetaan käyttäjälle ymmärrettävään muotoon ja kuultavaksi kaiutinvälineillä 25.1.

Kuvassa 4 on esitetty eräs esimerkki keksinnön mukaisen järjestelmän ohjelmointirajapinnoista salausjärjestelmän hallinnan yhteydessä. SIM-moduulin 28 e2e-osiolle 23 on järjestetty avaimien hallinta 28.2 (Key Management) ja SAT 21 . Päätelaitteen 11.1, 11.2 SIM-moduulille 28 tarjoama rajapinta voidaan kytkeä MIDdletin 27 MIDP:n yleiseen käyttäjärajapintaan. Tällöin ladattava MIDdlet 27 toteuttaa SIM-moduulille 28 rajapinnan, jonka kautta tämä voi ohjata päätelaitteen 11.1, 11.2 toimintaa. Tällöin siis SAT-funktiot on konvertoitu MIDP-API:n funktioiksi.

SIM-moduulin 28 e2e-osio 23 on SIM API:n 28.1 kautta yhteydessä Java®-MIDdletissä 27 toteutettuun SAT:iin 21. MIDdletin 27 SAT 21' on Messaging API -rajapinnan 35 kautta yhteydessä TNSDS-SAP:iin 31 (TETRA SDS Service Access Point). TNSDS-SAP 31 on protokolla, jolla käyttäjäsovellukset, pääsevät hyödyntämään SDS-siirtokantajaa. Datalähetys ja -vastaanotto voidaan suorittaa SDS:n ohella SMS:nä (Short Message Service), kuten GSM:ssä.

Erään edullisen sovellusmuodon mukaan myös päätelaitteelle 11.1, 11.2 ladattu sovellus 27 voi sen lisäksi, että se toteuttaa SIM-moduulille 28 rajapinnan, ohjata myös itsenäisestikin päätelaitteen 11.1, 11.2 toimintaa ohjelmointirajapinnan 36 kautta. Tällöin päätelaitteelle 11.1, 11.2 ladatulla sovelluksella 27 mahdollistetaan päätelaitteelle SAT-toiminnallisuus 21', käyttäen päätelaitteessa 11.1, 11.2 olevaa ohjelmointirajapintaa 36 (MIDP-API). Yleisesti tämä ominaisuus on erittäin käyttökelpoinen eikä se näin ollen ole mitenkään pelkästään päästä-päähän -salausspesifinen.

Jos päätelaitteelle 11.1, 11.2 lähetettävä SDS-data on esimerkiksi salausavaimia tai -sovelluksia MIDdlet:in 27 SAT 21' käsittelee ja ohjaa nämä silloin SIM-moduulille 28 SIM API:n 28.1 viestiprotokollan 28* läpi. SIM-moduulilla 28 sanottua salausinformaatiota käsitellään siten, kuin edellä on kuvattu.

Jos SDS-kantajan kautta tuleva informaatio on esimerkiksi kuvia, pelejä, animaatioita, ääniä ym. informaatiota, niin nämä ohjataan suoraan MIDP:n tavallista API:a 36 pitkin MIDdletistä 27 toteutetulta SAT:lta 21' päätelaitteen 11.1, 11.2 käyttäjärajapintaan, johon kuuluu esimerkiksi näppäimistö, näyttö ja kaiutin 25.1.

Päätelaitteella 11.1, 11.2 ajetaan siis dynaamista virtuaalisuoritinta KVM 20, jossa päästä päähän -salauksen ollessa aktiivisena sen toteuttavaa MIDdlet:iä 27 dynaamisella virtuaalisuorittimella 20 ajetaan. Jos päätelaitteen 11.1, 11.2 käyttäjä haluaa aktivoida jonkun muun Java®-sovelluksen, lopetetaan salaussovelluksen suoritus, jota seuraa ilmoitus käyttäjälle. Salaussovellusta voidaan ajaa mahdollisesti myös taustamoodissa mikäli päätelaitteen 11.1, 11.2 ja virtuaalisuorittimen resurssit sen vain sallivat.

Käyttäjärajapinnassa Middlet-salaussovellus 27 voidaan toteuttaa siten, että se on aina aktiivinen tai vaihtoehtoisesti käyttäjän erikseen aktivoitavissa. Sovelluksen 27 ollessa asetettuna aina aktiiviseksi, sen aktivointi tapahtuu automaattisesti päätelaitteen 11.1, 11.2 kytkeytyessä päälle. Päätelaitteessa 11.1, 11.2 voi olla yksi tai useampia sovelluksia, jolloin ne tarvitsevat jonkinlaisen erottimen muista mahdollisista sovelluksista erottamiseksi.

Käyttäjävalinnainen toteutustapa on tuttu esimerkiksi GSM-päätelaitteista. Siinä käyttäjä voi aktivoida haluamansa sovelluksen Java-sovellusvalikossa. Middlet-sovelluksen tulosteet (valikot, graafiset elementit, ym.) esitetään edullisimmin esimerkiksi alivalikkona, koska muutoin ne saattavat aiheuttaa sekaannusta päätelaitteen varsinaiseen käyttäjärajapintaan UI. Normaalissa käyttäjärajapinnassa voidaan esittää esimerkiksi jokin ikoni, jonka kautta päästään MIDdlet-sovellusmenuun.

Ajettavissa olevia sovelluksia voidaan myös luokitella eri kriteerien mukaisesti. Tällöin voidaan asettaa erikoisoikeudet esimerkiksi juuri keksinnön mukaiselle salaussovellukselle.

Keksinnön mukainen järjestelmä tarjoaa päätelaitteen 11.1, 11.2 käyttäjäryhmille merkittävän parannuksen salausinformaation turvaominaisuuksiin. Käyttäjäryhmä voi esimerkiksi vaihtaa avaimia pidemmiksi omien tarpeidensa mukaan, jolla voidaan kasvattaa merkittävästi salauksen turvallisuutta.

On ymmärrettävä, että edellä oleva selitys ja siihen liittyvät kuvat on tarkoitettu ainoastaan havainnollistamaan esillä olevaa keksinnön mukaista järjestelmää. Keksintöä ei siten ole rajattu pelkästään edellä esitettyihin tai patenttivaatimuksissa määriteltyihin suoritusmuotoihin, vaan alan ammattimiehelle tulevat olemaan ilmeisiä monet erilaiset keksinnön variaatiot ja muunnokset, jotka ovat mahdollisia oheisten patenttivaatimusten määrittelemän keksinnöllisen ajatuksen puitteissa.

L3

PATENTTIVAATIMUKSET

1. Järjestelmä digitaalisessa langattomassa tiedonsiirtoverkossa (10) päästä päähän (e2e) -salauksen järjestämiseksi, erityisesti audiomuotoiselle lähetykselle, jossa tiedonsiirtoverkossa (10) viestii keskenään kaksi tai useampia päätelaitteita (11.1, 11.2), joihin kuuluu ainakin

- koodekki (24) analogisen audiosignaalin muuntamiseksi datavirraksi ja päin vastoin,
- ilmatiesalausvälineet (19, 30),
- välineet (28) päätelaitteen (11.1, 11.2) yhteyteen tallennettujen salausparametrien (TEK, IV) hallinnoimiseksi
- salausavaingeneraattori KSG (23) käyttöavaimen (KSS) luomiseksi sanotuilla salausparametreilla (TEK, IV),
- välineet (20) datavirran salaamiseksi ja salauksen purkamiseksi luodulla käyttöavaimella (KSS, IV),
- välineet (33.1, 33.2) salatun datavirran synkronoimiseksi ja synkronoinnin purkamiseksi ja
- ainakin yksi rajapinta (19) salausparametrien vastaanottamiseksi tiedonsiirtoverkosta (10),

ja jossa ainakin yksi tiedonsiirtoverkkoon (10) kuuluvista päätelaitteista on sovitettu toimimaan erityisenä palvelinpäätelaitteena (15), joka hallinnoi ja jakaa ainakin tiedonsiirtoverkkoa koskevia salausparametreja (19) muille päätelaitteille (11.1, 11.2) asetetun kriteerin perusteella, <u>tunnettu</u> siitä, että

- sanottu erityinen palvelinpäätelaite (15) on lisäksi järjestetty hallinnoimaan ainakin salaus- ja synkronointisovelluksia (32) ja jakamaan niitä asetetun kriteerin perusteella muille päätelaitteille (11.1, 11.2) ja
- päätelaiteisiin (11.1, 11.2) on järjestetty toiminnallisuudet (21, 22) sanottujen sovelluksien (32) lataamiseksi ja hallitsemiseksi sekä
- datamuistia (23) sovelluksien (32) tallentamiseksi ja

- suoritin (20) ja käyttömuistia sovelluksien (32) suorittamiseksi.

2. Patenttivaatimuksen 1 mukainen järjestelmä, tunnettu siitä, että päätelaite (11.1, 11.2) on sovitettu ajamaan sanotulla suorittimella (20) J2ME- (Java 2 Platform Micro Edition) spesifikaation mukaisia sovelluksia (32).

3. Patenttivaatimuksen 2 mukainen järjestelmä, tunnettu siitä, että päätelaite (11.1, 11.2) on konfiguroitu MIDP- (Mobile Information Device Profile) spesifikaation mukaiseksi.

4. Jonkin patenttivaatimuksen 1 - 3 mukainen järjestelmä, tunnettu siitä, että sovelluksien (32) lataaminen päätelaitteelle (11.1, 11.2) on järjestetty tapahtumaan itseorganisoituvasti, kuten esimerkiksi SDS-viesteinä (Short Data Service).

5. Digitaalinen langaton päätelaite (11.1, 11.2), johon kuuluu toiminnallisuudet ainakin

- moduuli (20) salauksen toteuttamiseksi,
- yksi tai useampia moduuleja (33.1, 33.2) synkronoinnin toteuttamiseksi ja
- moduuli (21, 28) ainakin salausavaimien (TEK) vastaanottamiseksi ja hallitsemiseksi, tunnettu siitä, että

ainakin yhden moduulin (20, 33.1, 33.2, 21) toiminnallisuus on sovitettu toteutettavaksi dynaamisella sovelluksella (27) ohjelmallisesti.

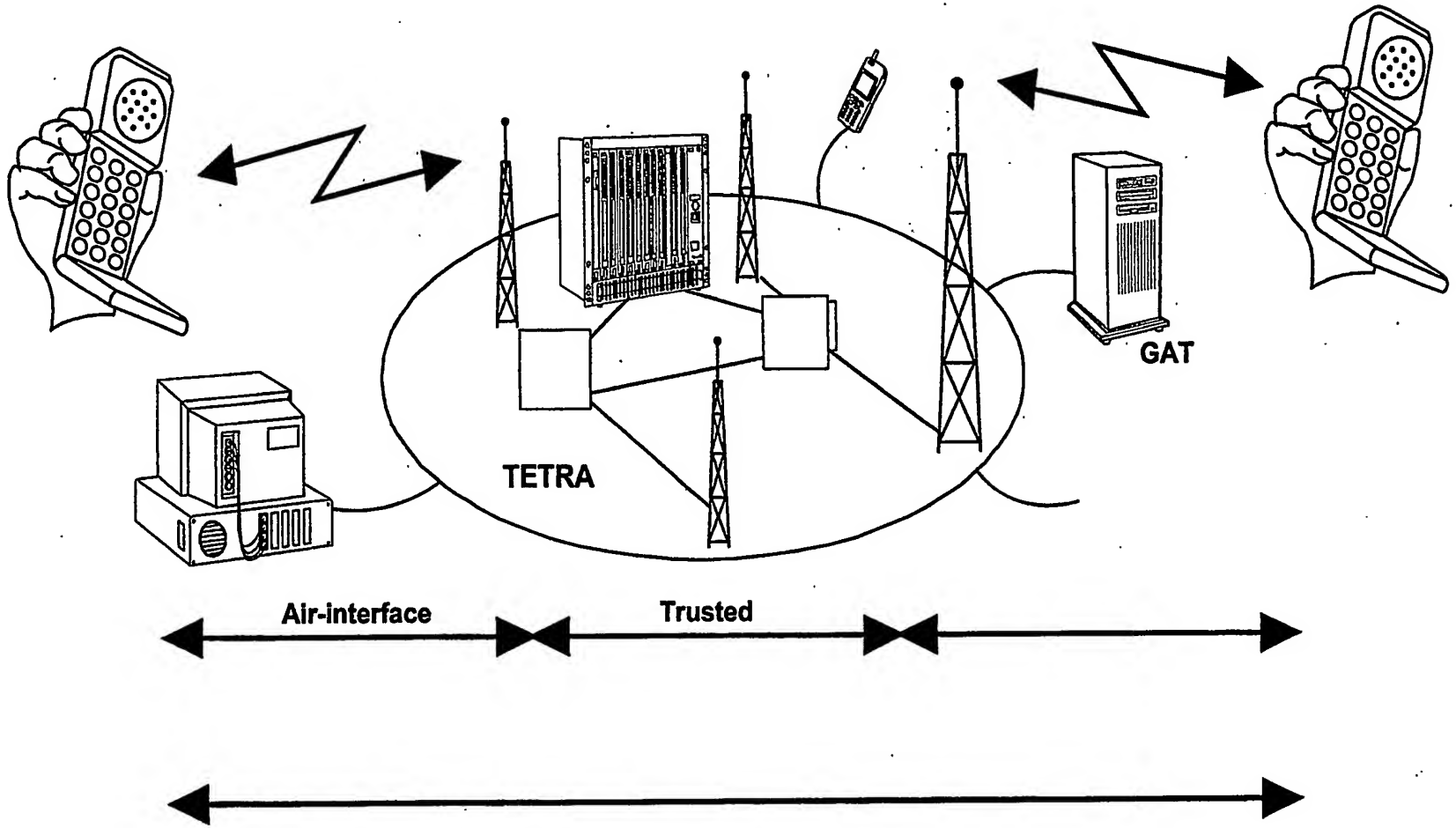
6. Patenttivaatimuksen 5 mukainen päätelaite (11.1, 11.2), johon kuuluu ainakin SIM-moduuli (28), tunnettu siitä, että sanottu sovellus (27) on sovitettu järjestämään ainakin SIM-moduulin (28) ja päätelaitteen (11.1, 11.2) väliselle rajapinnalle komentotoiminnallisuuden (21') sovelluksen (27) ohjelmointirajapinnan (MIDP API) kautta.

(57) TIIVISTELMÄ

Keksintö koskee järjestelmää digitaalisessa langattomassa tiedonsiirtoverkossa (10) päästä päähän (e2e) -salauksen järjestämiseksi, erityisesti audiomuotoiselle lähetykselle. Tiedonsiirtoverkossa (10) viestii keskenään kaksi tai useampia päätelaitteita (11.1, 11.2), joihin kuuluu ainakin
- koodekki (24) analogisen audiosignaalin muuntamiseksi datavirraksi ja päin vastoin,
- ilmatiesalausvälineet (19, 30),
- välineet (28) päätelaitteen (11.1, 11.2) yhteyteen tallennettujen salausparametrien (TEK, IV) hallinnoimiseksi
- salausavaingeneraattori KSG (23) käyttöavaimen (KSS) luomiseksi sanotuilla salausparametreilla (TEK, IV),
- välineet (20) datavirran salaamiseksi ja salauksen purkamiseksi luodulla käyttöavaimella (KSS, IV),
- välineet (33.1, 33.2) salatun datavirran synkronoimiseksi ja synkronoinnin purkamiseksi ja
- ainakin yksi rajapinta (19) salausparametrien vastaanottamiseksi tiedonsiirtoverkosta (10).

Ainakin yksi tiedonsiirtoverkkoon (10) kuuluvista päätelaitteista on sovitettu toimimaan erityisenä palvelinpäätelaitteena (15), joka hallinnoi ja jakaa ainakin tiedonsiirtoverkkoa koskevia salausparametreja (19) muille päätelaitteille (11.1, 11.2) asetetun kriteerin perusteella. Sanottu erityinen palvelinpäätelaite (15) on lisäksi järjestetty hallinnoimaan ainakin salaus- ja synkronointisovelluksia (32) ja jakamaan niitä

asetetun kriteerin perusteella muille päätelaitteille (11.1, 11.2) ja päätelaiteisiin (11.1, 11.2) on järjestetty toiminnallisuudet (21, 22) sanottujen sovelluksien (32) lataamiseksi ja hallitsemiseksi sekä datamuistia (23) sovelluksien (32) tallentamiseksi ja suoritin (20) ja käyttömuistia sovelluksien (32) suorittamiseksi.


GAT
TETRA
Air-interface
Trusted